TechXplore

NIST releases version 2.0 of cybersecurity framework

February 27 2024

TRAVELING THROUGH NIST'S
CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES
CSF 2.0
For industry, government, and organizations to reduce cybersecurity risks

Credit: Natasha Hanacek, NIST

The National Institute of Standards and Technology (NIST) has updated the widely used Cybersecurity Framework (CSF), its landmark guidance document for reducing cybersecurity risk. The new 2.0 edition is designed for all audiences, industry sectors and organization types, from the smallest schools and nonprofits to the largest agencies and corporations—regardless of their degree of cybersecurity sophistication.

In response to the numerous comments received on the draft version, NIST has expanded the CSF's core guidance and developed related resources to help users get the most out of the framework. These resources are designed to provide different audiences with tailored pathways into the CSF and make the framework easier to put into action.

"The CSF has been a vital tool for many organizations, helping them anticipate and deal with cybersecurity threats," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "CSF 2.0, which builds on previous versions, is not just about one document. It is about a suite of resources that can be customized and used individually or in combination over time as an organization's cybersecurity needs change and its capabilities evolve."

The CSF 2.0, which supports implementation of the National Cybersecurity Strategy, has an expanded scope that goes beyond protecting critical infrastructure, such as hospitals and power plants, to all organizations in any sector. It also has a new focus on governance, which encompasses how organizations make and carry out informed decisions on cybersecurity strategy. The CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should consider alongside others such as finance and reputation.

"Developed by working closely with stakeholders and reflecting the most recent cybersecurity challenges and management practices, this update aims to make the framework even more relevant to a wider swath of users in the United States and abroad," according to Kevin Stine, chief of NIST's Applied Cybersecurity Division.

Following a presidential Executive Order, NIST first released the CSF in 2014 to help organizations understand, reduce and communicate about cybersecurity risk. The framework's core is now organized around six key functions: Identify, Protect, Detect, Respond and Recover, along with CSF 2.0's newly added Govern function. When considered together, these functions provide a comprehensive view of the life cycle for managing cybersecurity risk.

The updated framework anticipates that organizations will come to the CSF with varying needs and degrees of experience implementing cybersecurity tools. New adopters can learn from other users' successes and select their topic of interest from a new set of implementation examples and quick-start guides designed for specific types of users, such as small businesses, enterprise risk managers, and organizations seeking to secure their supply chains.

A new CSF 2.0 Reference Tool now simplifies the way organizations can implement the CSF, allowing users to browse, search and export data and details from the CSF's core guidance in human-consumable and machine-readable formats.

In addition, the CSF 2.0 offers a searchable catalog of informative references that shows how their current actions map onto the CSF. This catalog allows an organization to cross-reference the CSF's guidance to more than 50 other cybersecurity documents, including others from NIST, such as SP 800-53 Rev. 5, a catalog of tools (called controls) for achieving specific cybersecurity outcomes.

Organizations can also consult the Cybersecurity and Privacy Reference Tool (CPRT), which contains an interrelated, browsable and downloadable set of NIST guidance documents that contextualizes these NIST resources, including the CSF, with other popular resources. And the CPRT offers ways to communicate these ideas to both technical experts and the C-suite, so that all levels of an organization can stay coordinated.

NIST plans to continue enhancing its resources and making the CSF an even more helpful resource to a broader set of users, Stine said, and feedback from the community will be crucial.

"As users customize the CSF, we hope they will share their examples and successes, because that will allow us to amplify their experiences and help others," he said. "That will help organizations, sectors and even entire nations better understand and manage their cybersecurity risk."

This story is republished courtesy of NIST. Read the original story here.

Provided by National Institute of Standards and Technology

Citation: NIST releases version 2.0 of cybersecurity framework (2024, February 27) retrieved 11 May 2024 from https://techxplore.com/news/2024-02-nist-version-cybersecurity-framework.html